



2020 年度 互联网企业 信息科技风险治理 现状调研报告

中国互联网协会信息技术（IT）风险治理工作委员会

2021 年 2 月

VISIT...

LANZAROTE
Caliente.COM

版权声明

本调研报告版权属于中国互联网协会信息技术（IT）风险治理工作委员会，并受法律保护。转载、摘编或利用其它方式使用本调研报告文字或者观点的，应注明“来源：中国互联网协会信息技术（IT）风险治理工作委员会”。违反上述声明者，将追究其相关法律责任。

目录



01

调研背景

为深入洞察互联网企业信息科技风险治理面临的主要风险、治理现状以及存在的痛点和挑战，中国互联网协会信息技术（IT）风险治理工作委员会发起了《互联网企业信息科技风险治理现状调查问卷》。本报告由问卷调查结果汇总整理而成，旨在协助互联网企业掌握行业信息科技风险治理动态，对标行业最佳实践，为企业建立有效的信息科技风险治理体系奠定基础。

本次调研共收回 62 份有效的问卷样本，覆盖了超过三十种业务类型的互联网企业。问卷参与者主要来自互联网企业信息技术部门（29%），安全部门（16%）和业务部门（10%），其余包括内控部门、法律合规部门、政府公共事务部门等。

本次调研的受访者来自运营不同类型业务的互联网企业，主要涵盖生活服务类、设备设施类、大众消费类、商业服务类等业务领域，调研范围具有广泛性（见表 1）。

贵公司开展的主营业务包括以下哪些？		
选项	小计	比例
即时通讯	6	9.68%
搜索引擎	7	11.29%
网络新闻	10	16.13%
网络视频	13	20.97%
网络购物	10	16.13%
第三方支付	12	19.35%
电子商务	15	24.19%
互联网金融	16	25.81%
网络零售	8	12.90%
网络广告	16	25.81%
网络教育	8	12.90%
网络游戏	10	16.13%
社区	8	12.90%
传统媒体网络版	4	6.45%
自媒体平台	4	6.45%
共享经济	3	4.84%
其他	22	35.48%

表 1 互联网企业业务分布统计

本次调研从员工数量和营业收入两个方面对不同规模的互联网企业进行统计，调研样本较为全面（见图 1 和图 2）。

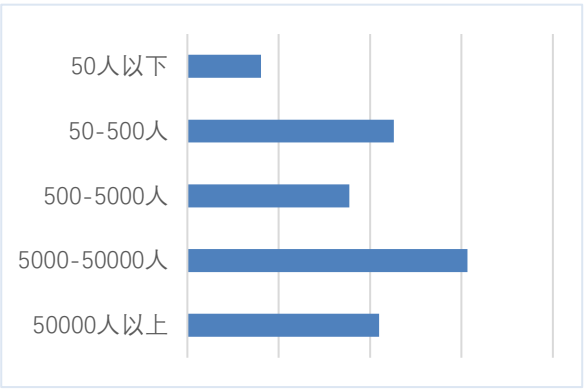


图 1. 互联网企业人员规模统计

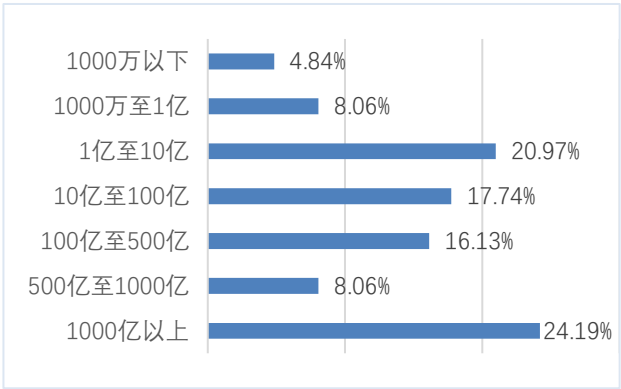


图 2. 企业营业规模（年营业收入：人民币）统计

根据调研结果显示，超过 88.7%的受访者所在企业的主营业务受工业和信息化部监管(见图 3)。此外，受经营范围影响，部分互联网企业还同时受到国家广播电视总局、中国人民银行、银行保险监督管理委员会、国家广播总局等机构监管。

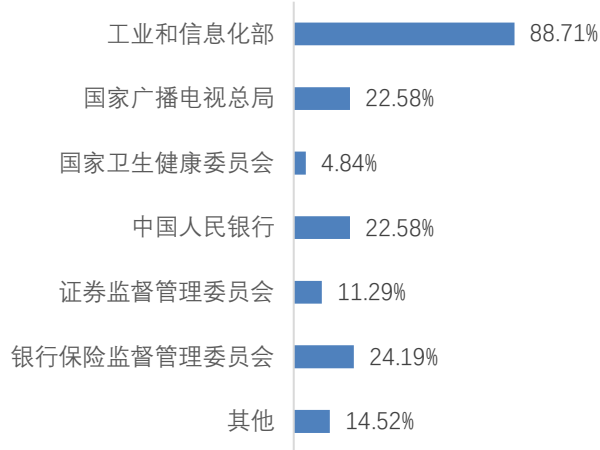


图 3. 互联网企业主营业务的监管机构分布

在受访者所在企业中，占比最大的是非上市公司，约为 54%。此外，美股上市公司占比 19.35%，港股上市公司占比 12.9%，国内上市公司占比 17.74%。

参与本次调研的互联网企业中约 43.5%已开展出海业务，涉及全球多个国家和地区（见图 4）。其中，在欧盟成员国开城的企业占比最多，超过了 66%。其次是美国（62.96%）和俄罗斯（55.56%）。除此之外，还有部分互联网企业选择在日本、印度、新加坡、马来西亚、澳大利亚等国家开城。

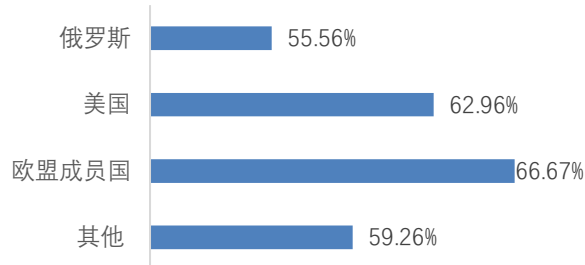


图 4. 跨境业务涉及的主要国家或地区统计



02

现状概述

治理组织架构

治理组织架构是企业开展信息科技风险治理工作的基础。根据调研我们发现，参与调研的大部分互联网企业设立了信息科技风险治理责任部门，其中，68%的受访企业已明确信息科技风险治理的实体责任部门，主要由风险、安全、合规、内控、法务等部门承担。18%的受访企业以跨部门的工作委员会形式开展工作。此外，14%的受访企业反馈尚未设立明确的责任部门，根据统计分析我们发现，尚未设立明确的责任部门的企业普遍规模较小，且非上市公司。

调研结果显示，仅有 29.03%的企业设置了首席风险官（CRO）。而在信息科技风险治理责任人方面（见图5），由首席信息官（CIO）、首席信息安全官（CISO）承担企业信息科技风险治理责任的情况较多（18.18%），此外，部分企业由公司法人（13.64%）、首席执行官（CEO）（15.91%）、业务条线负责人（15.91%）承担信息科技风险治理责任，首席风险官（CRO）、首席技术官（CTO）占比较少，另外少数企业尚未明确信息科技风险治理责任人。这体现出部分互联网企业仍未形成职责明确、相互制衡的信息科技治理组织架构，风险管理责任人同时承担经营管理和决策，对风险管理工作的独立性有一定影响。

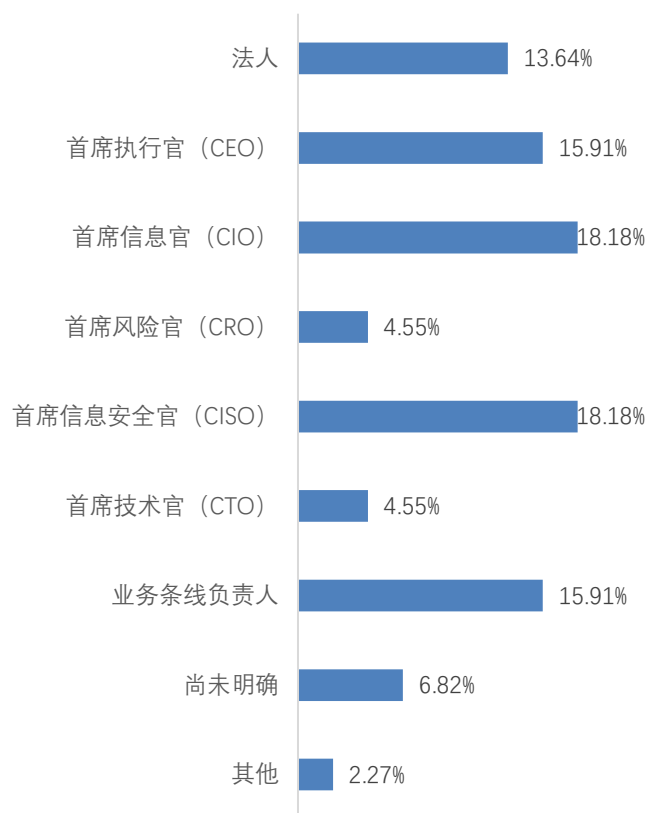


图 5. 互联网企业信息科技风险治理的第一责任人统计



风险管理策略

问卷针对互联网企业信息科技风险治理目标进行了调研。调研结果显示**互联网企业开展信息科技风险治理活动最主要的目标是为了保障业务正常运行（83.87%）和防范信息科技风险事件（85.48%）**，其次是为了符合监管合规要求（82.26%）。对比以上，较少企业将承担社会责任（64.52%）和获取资质（46.77%）作为主要的风险治理目标。

从面临的主要风险来源来看（见图6），受访者所在互联网企业普遍认为来自合作伙伴、软硬件供应商、外包服务商和同业企业的生态风险最高（61.13%）。其次是来自于人员有意或无意的违规操作（56.45%）与不符合法律法规和监管要求（41.94%）的风险。来自信息系统软硬件缺陷和管理制度流程缺失的风险相对较少，分别为32.26%和35.48%。**生态风险**

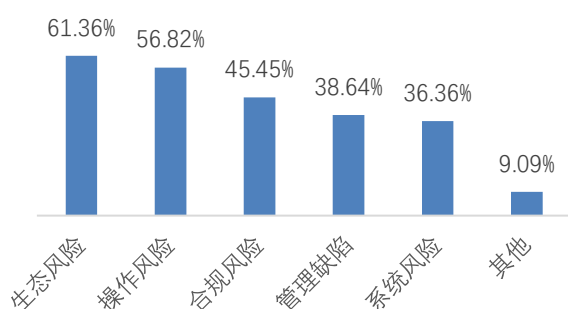


图6. 互联网企业风险来源分布

和操作风险是受访互联网企业面临主要的风险来源。

互联网企业开展信息科技风险治理活动的过程中存在各种各样的痛点和挑战，在本次调研中，我们发现**企业开展信息科技风险治理活动最主要的挑战是员工风险意识不足**。除此之外，缺少风险管理框架、风险管理边界不清晰也是普遍存在的问题（38.71%）。部分企业还存在缺少预算、人员专业知识技能不足的问题，业务部门配合度低也成为企业开展风险治理活动的困难和挑战。

同时，通过统计分析和对比，我们发现规模不同的企业存在的痛点和挑战也有所不同。规模较大的企业更加倾向于认为业务部门的配合度不高和员工意识不足是推动信息科技风险治理工作的主要挑战。而规模较小的企业的痛点更加集中表现为缺少预算和风险管理框架（见图7）。

备注：本文中所称信息科技风险是指在互联网企业的业务运营、内部管理等方

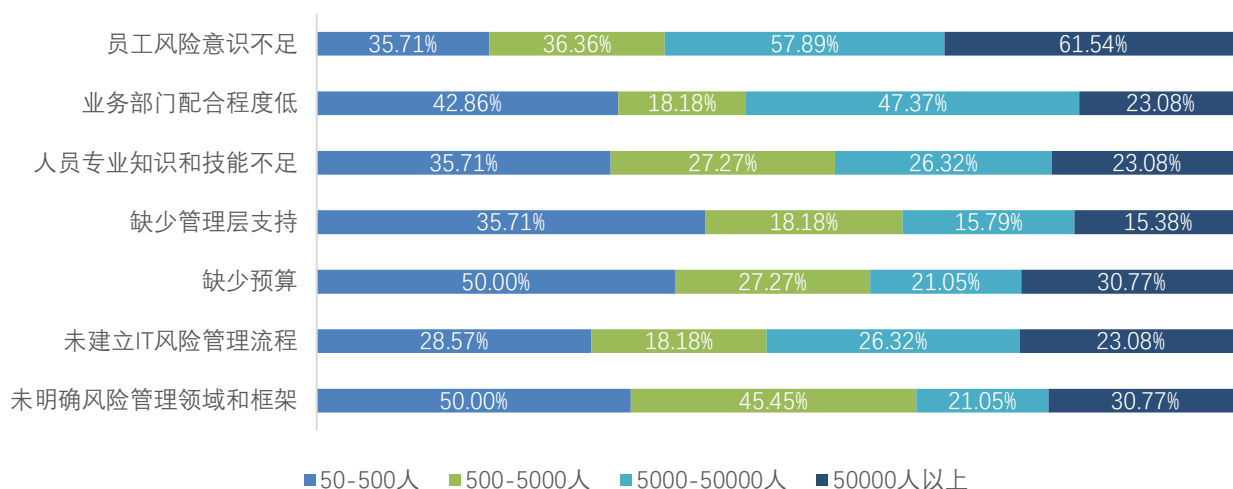


图7. 互联网企业风险治理痛点和挑战

管理现状概述

我们从互联网行业普遍关注的十个治理领域^{*}开展调研，涵盖了法律合规、业务安全管理、个人信息保护、数据管理、内容治理、应用管理、平台管理、基础设施运行、生态建设、新技术应用。

在本次调研中，我们邀请受访者为其所在企业在各个领域开展风险治理活动的成熟度进行评分（见图8）。从自评结果来看，受访者普遍认为其风险治理水平能够满足基本管理需求，但距离目标还存在一定差距。其中，法律合规、个人信息保护、数据管理、基础设施运行等领域的风险治理成熟度较高，生态建设和新技术应用领域的成熟度较低。

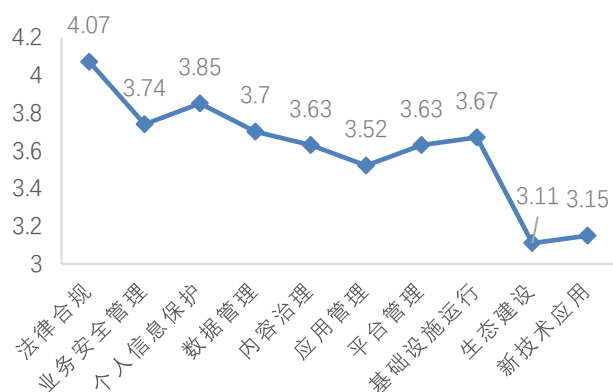


图8. 互联网企业信息科技风险治理活动成熟度自评分

从迫切程度来看（见图9），互联网企业认为最迫切需要开展风险治理活动的领域为个人信息保护

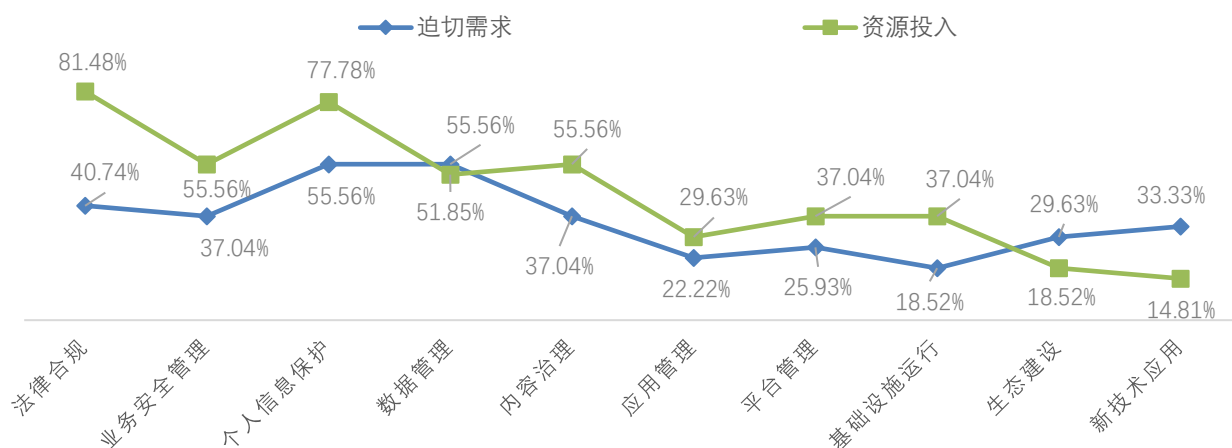


图9. 互联网企业信息科技风险治理存在迫切需求的领域和资源投入情况统计分析

（51.61%）和数据管理（46.77%）。其次为新技术应用（38.71%）、业务安全管理（35.48%）和法律合规（33.87%）。优先级较低的领域包含应用管理和基础设施运行，分别为22.58%和19.35%。

从资源投入来看，互联网企业在数据管理（61.29%）、个人信息保护（59.68）、法律合规（58.06%）和业务安全管理（48.39%）领域的高投入最为普遍。然而，目前企业在生态建设（8.06%）和新技术应用领域（16.13%）的投入普遍较低。

备注：在本次调研中将互联网信息科技风险治理活动分为十个主要领域：

- ① 法律合规领域涵盖了法律、行政法规、行业准则的符合情况；
- ② 数据管理领域涵盖了数据质量管理，数据安全等内容；
- ③ 个人信息保护领域涵盖了数据隐私影响分析，数据主体权力，告知同意等内容；
- ④ 业务安全管理领域涵盖了对网络欺诈、作弊套利等业务安全的防控；
- ⑤ 内容治理领域涵盖了内容审查、用户管理、不良信息管理等内容；
- ⑥ 应用管理领域涵盖应用安全、接口管理、开发运维等内容；
- ⑦ 基础设施运行涵盖了IT基础设施、网络安全、业务连续性等内容；
- ⑧ 平台管理领域涵盖了数据平台、运维服务等跨业务条线提供服务的企业中台；
- ⑨ 生态建设领域涵盖了供应商管理、合作伙伴管理、外包服务管理、开源组件管理等内容；
- ⑩ 新技术应用领域涵盖了对新技术引入所带来的技术风险及衍生风险的影响评估和管控等。

同时，我们对各风险治理领域涉及的监管要求、行业规范以及管理标准进行了调研（见图 10）。根据调研结果我们发现，互联网企业普遍反馈在生态建设，以及人工智能、区块链、大数据等新技术应用领域较为空白，缺少指引和规范。因此可能导致互联网企业难以有效地实施可落地的风险治理措施防范行业生态和新技术带来的新风险。

除以上各领域风险治理活动的开展情况外，我们还统计了目前互联网企业获得的资质认证情况。调研结果显示，监管合规仍是互联网企业获取资质认证的主要驱动力，已有约 70% 的受访企业通过了网络安全等级保护测评。在其他国内外认证中，ISO/IEC 27001 成为目前互联网企业获得最多的资质认证，占比超过 65%。而其他类型的资质认证在受访的互联网企业中并不具备普遍性。

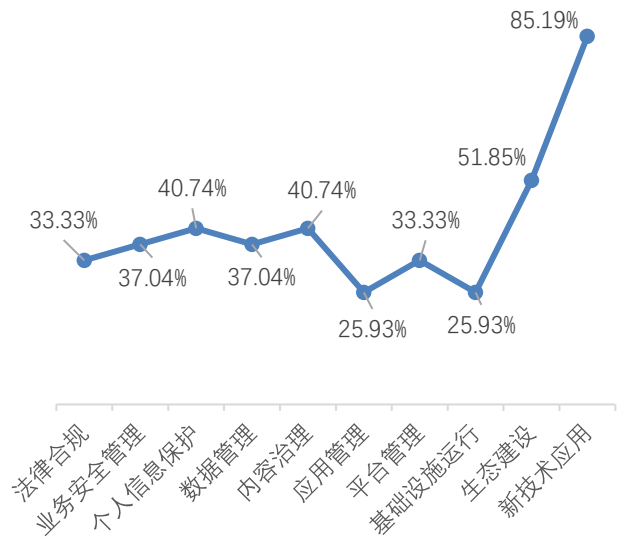


图 10. 互联网企业信息科技风险治理缺少指引和规范的领域统计





为了进一步掌握互联网企业在各个重点领域的风险治理现状，我们通过问卷对重点领域进行了详细调研，并对反馈结果进行了统计分析，希望能够发现互联网企业在各重点领域的发展特征和共性问题，为后续开展风险治理工作指导方向。

法律合规管理领域

近年来，我国网络空间法治不断推进，互联网企业所面临的信息科技法律体系日趋完善，以《网络安全法》为代表的网络安全立法顶层设计已基本完成，随着《数据安全法（草案）》、《个人信息保护法（草案）》的陆续发布，即将填补了我国数据安全方面的空白，也进一步构建了网络安全管理框架。《网络信息内容生态治理规定》的出台、《未成年保护法》新增“网络保护”章节，标志着互联网执法、司法体系不断提高。

另一方面，个人信息保护一直是全球的热点话题，已有超过 140 个国家和地区正在开展个人信息保护立法工作，大幅度提升了互联网企业出海的合规门槛。

因此，法律合规工作是互联网企业不可或缺的重要组成部分。调研结果显示，93.48%的受访企业已设立独立的部门承担法律合规工作。而剩余 6.52%尚未设立法律合规部门的企业均为员工数量小于 500 的规模较小的企业。

从调研结果来看，个人信息保护与数据安全方面的法律合规已经引起了互联网企业的高度重视，其中 93.48%的互联网企业已将个人信息保护作为企业法律合规重点，其次是业务安全管理与数据管理，占

比均超过了 70%。

在开展法律合规工作中，对法律、行业规范和准则的追踪不及时（32.61%）、解读不准确（32.61%）并不是互联网公司面临的主要困难。根据调研结果显示，50%的受访者所在企业认为**难以根据法律法规准确评估企业运营现状是否符合合规要求才是现阶段最大的痛点**。

除此之外，与信息科技风险治理整体情况相同，互联网企业法律合规工作过程存在的困难仍以人员因素为主，认为“**法律合规专业人员缺少信息科技相关专业知识的受访者占比为 50%**”。

在合规工具方面，超过 60%的互联网企业部署的合规工具仅用于收集汇总法律合规文件，39.13%的企业形成了法律知识合规知识库。仅有 21.74%的企业运用了智能化合规风险监测工具。**这表明互联网企业法律合规工具普遍停留在基础法律文件的收集和管理层面，距离自动化、智能化地监测、评估和处置企业合规风险还有一定发展空间。**

业务安全管理领域

在需要开展业务安全风险治理的企业中，由安全部门开展业务安全管理的占比最高（60.98%），其次是法律合规部门（58.54%）与业务部门（51.22%），风险管理部门、内控部门和审计部门也都涉及业务安全管理。

在业务安全管理工作开展过程中，大部分的受访者认为企业的主要挑战为难以有效地识别和防范业务策略漏洞，而在技术漏洞和管理漏洞的识别方面，受访者普遍认为企业表现较为良好。

此外，业务安全管理通常依赖于业务风控平台，根据调研结果显示，73.17%的受访企业自行研发了风控平台，17.07%的企业采用外购的服务平台，另外还有9.76%的企业尚未应用平台技术来管控业务安全。这说明互联网企业拥有较强的研发能力，其业务风控平台多以自开发为主。通过自动化、智能化技术手段开展业务安全风控是互联网企业的主要趋势。





个人信息保护领域

在关注个人信息保护领域的企业中，90.48%的受访者认为其所在公司已经明确了个人信息保护责任人。其中，26.19%的企业明确个人信息保护责任部门为法律合规部门，28.57%的企业为信息安全部门，14.29%为数据管理部门，跨条线的工作委员会占比16.67%。

从企业开展个人信息保护活动来看，超过90%的企业已对个人信息处理活动进行了记录，然而其中约23%的受访者认为企业在定期维护和更新记录方面存在困难。此外，超过80%的企业已建立个人信息保护政策和个人信息泄露应急处置预案，76.19%的受访者表示企业已开展个人信息安全影响评估。相较以上活动，受访者反馈的信息显示企业在个人信息保护自动化合规检查（40.48%）和个人信息保护审计（54.76%）方面开展的活动较少。

整体来看，大多数互联网企业已积极采取活动开展个人信息保护。在组织架构、管理政策和流程方面已建立较为完善的解决方案，而在搭建自动化的工具平台和审计活动方面相对滞后。

数据管理领域

根据调研结果显示，在数据质量管理方面已有超过50%的企业制定了企业级数据标准，实现了采集阶段的数据校验，并认为对于发现的数据质量问题能够及时整改。然而，仅有约35%的受访者认为其所涉及企业的数据质量足够支持数据价值实现。这表明虽然大部分企业已认识到数据管理的重要性，采取了积极的应对措施，然而目前企业数据质量对于支撑数据价值的充分实现仍有进一步提升空间。

在数据安全方面，超过80%的企业已开展数据生命周期安全管理。约90%的企业已制定数据分类分级方法，然而24.44%的企业尚未根据分类分级方法对数据进行标识。在数据安全技术工具方面，数据防泄漏工具、全站加密传输、敏感信息加密存储、运维堡垒机以及密钥管理系统等数据安全解决方案在互联网企业应用较多。

内容治理领域

在开展网络内容服务的企业中，74.19%已设立网络内容生态治理负责人。在网络信息内容审查人员规模方面，大部分企业审查人员团队维持在千人以下，但也有 6.45%的企业配置了超过万人的审查团队，这体现出**网络信息内容服务平台在内容管理方面非常重视，资源投入高**。

调研结果显示，在内容治理措施方面，建立用户账号管理体系（占比 90.32%）、实时巡查平台内容（占比 87.1%）等方式较为普及，多级人员审核和技术审核也是目前企业普遍采取的内容审核机制（占比 77.4%）。同时，超过 90%的受访者反馈企业已在网络信息内容服务平台设立了投诉举报渠道。但是，针对未成年人的保护措施目前仍比较欠缺（仅 48.39%）。

应用管理领域

目前敏捷开发已成为互联网企业应用开发的主要模式。在涉及应用管理领域的企业中，30.30%的企业已由公司统一制定敏捷开发政策和细则。此外，45.45%的企业已在公司层面制定政策，由各事业部基于政策制定可落地的管理细则。然而约有 25%的受访者认为企业敏捷开发管理制度方面存在不足。

根据调研结果显示，分别有超过 90.91%和超过 75.76%的受访者认为其所在企业已在软件开发需求阶段考虑到隐私和安全方面的要求。**这表明互联网企业已逐步落实 Privacy by Design 和 Security by Design 的管理思路**。

平台管理领域

随着互联网企业管理架构不断地发展和调整，实现内部资源共享或集中化管理的平台服务也逐渐成为互联网企业建设的重点。根据调研结果显示，大部分受访者所在企业均涉及对于数据平台、风控平台、运维平台、云平台、开发平台的管理活动。





基础设施运行领域

调研结果显示，64.10%的互联网企业使用自建的数据中心，76.92%的企业使用了 IDC 机房，38.46%的企业使用了外部的云服务。这表明部分互联网企业采用混合模式，既运营自己的 IT 基础设施，也使用外部资源。

根据统计，渗透测试和漏洞扫描是企业开展的最为普通的网络安全活动（超过 94%的企业均开展了上述活动）。相比之下，仅有 61.54%的受访者表示其所在企业开展了红蓝对抗等网络安全活动。

生态建设领域

受访者认为其所在企业在业务合作和软硬件供应方面较依赖第三方资源，而在系统开发、运维和数据处理活动方面自主性较高。同时，调研结果显示受访者中仅有 35.48%的互联网企业在生态建设领域开展了风险治理活动。从已开展生态建设风险治理活动的企业来看，分别有 81.82%和 77.27%的互联网企业已建立供应商和外包服务管理机制，而对于合作伙伴（64.64%）和开源组件（59.09%）的管理较为薄弱。互联网生态环境对于互联网企业的健康发展有着重要影响，大多数企业在内部信息科技风险治理工作中对于生态风险的管理和防范意识还有待加强提高。

新技术应用领域

目前开展新技术应用的企业中，大数据（89.66%）、人工智能（72.41%）、云计算（82.76%）仍是互联网应用较为普及的新技术，区块链（52.72%）、物联网（41.38%）等新技术应用较少。根据调研结果显示，96.55%的受访者认为其所在企业在引入新技术时开展了影响分析和风险评估，然而在新技术引入的新风险的应对方面，目前较为欠缺体系化、标准化的解决方案。

近年来，随着中国互联网行业的不断创新和高速发展，互联网企业对于国计民生的重要性也与日俱增。在面对巨大机遇的同时，互联网企业也看到了越来越严峻的风险形势和治理需求。

根据问卷调研结果显示，参与调研的互联网企业普遍已经在法律合规、个人信息保护、数据管理、内容治理、应用管理、基础设施运行等领域开展了信息科技风险活动。同时，通过调研，我们也总结出互联网企业在开展信息科技风险治理活动的过程中存在以下具有行业共性的发展特征和关键挑战。

部分互联网企业尚未形成职责明确、相互制衡的信息科技治理架构。在互联网企业发展前期，业务发展迅速，风险治理往往相对滞后。根据调研结果显示，部分互联网企业尚未建立起权、责、利对等的治理组织架构，科技风险管理缺少独立性和管理层支持，使得工作推进存在重重困难。

数据成为互联网企业信息科技风险治理的重点。随着线上业务飞速发展，网络用户数量和网络活动产生的数据量呈井喷式增长，数据资产已经成为互联网企业的基石与核心竞争力。近年来，全球已有超过 140 个国家和地区制定了个人信息保护法案，我国《网络安全法》、《数据安全法（草案）》、《个人信息保护法（草案）》等法律法规也陆续出台。因此，个人信息保护与数据管理既是监管合规重点关注的方向，也是行业风险集中的领域。调研结果显示互联网企业普遍在数据相关领域投入资源最多，开展信息科技风险活动也最为迫切。

互联网企业是“以科技治科技”的领军者，人员和生态因素成为科技风险治理的主要挑战。互联网企业具有领先的技术优势和自研水平，通常依赖技术管控措施的方式进行风险管理，因此对于能够利用技术方式管控的风险往往表现良好。然而根据调研结果显示，对于互联网企业来说，最常发生及难以防范的风险事件却并非来自于信息技术本身，而是来自于合作伙伴、供应商以及员工。

缺少针对新技术的风险管理指引和标准。互联网企业是创新的试验田，在业务和运营模式不断推陈出新的同时，也在积极探索大数据、人工智能、区块链等新兴技术的深度应用。新的技术不可避免地会带来新的风险，而对于企业如何调整机制有效地应对新风险，目前国内外均缺乏相关指引、标准和可落地的解决方案。

综合来看，中国互联网行业已经度过业务高速发展的初始阶段，迈入了稳定发展状态，企业应当回头审视自身的内部控制和风险管理水平，建立更加有效的治理架构，积极参与打造良好的生态环境。中国互联网协会信息技术（IT）治理工作委员会将持续跟进互联网企业信息科技风险治理发展状态，基于行业监管和企业需求，整合成员单位专家力量，共同制定具有可操作性和指导性的规范和标准，分享行业和领域最佳实践，推动行业生态建设，促进企业健康发展。



中国互联网协会

中国互联网协会是由国内从事互联网行业的网络运营商、服务提供商、设备制造商、系统集成商以及科研、教育机构等 70 多家互联网从业者共同发起成立，是由中国互联网行业及与互联网相关的企事业单位自愿结成的行业性的全国性的非营利性的社会组织，现有会员 1000 多个。中国互联网协会现任理事长为工业和信息化部原副部长、中国移动通信集团有限公司原董事长尚冰。协会的业务主管单位是工业和信息化部，会址设在北京市。中国互联网协会的宗旨是：以马克思列宁主义、毛泽东思想、邓小平理论、“三个代表”重要思想、科学发展观、习近平新时代中国特色社会主义思想为行动指南，贯彻落实创新、协调、绿色、开放、共享的发展理念，遵守宪法、法律、法规和国家政策，践行社会主义核心价值观，遵守社会道德风尚，坚持以创新的思维、协作的文化、开放的平台、有效的服务为指导思想，为会员需要服务，为行业发展服务，为政府决策服务，促进我国互联网事业的繁荣和发展，努力推进网络强国建设。

中国互联网协会信息技术（IT）风险治理工作委员会

中国互联网协会信息技术（IT）风险治理工作委员会是中国互联网协会下属非独立法人的二级分支机构，是由中国信息通信研究院、腾讯、阿里、华为、百度等多家单位共同发起成立，在信息技术（IT）风险治理领域开展研究和标准化工作。委员会将遵守国家法律、法规和行业规范，致力于搭建政府、企业和公众之间的桥梁，有效聚合产业界力量，推动信息技术（IT）风险治理工作不断发展，促进互联网信息技术（IT）风险治理领域交流与合作，支撑我国网络强国战略全面实施。